CybersÃ©curitÃ© : Que faire une fois victimes de cyberattaque
Internet
PostÃ© par : JerryG
PubliÃ©e le : 8/12/2023 13:00:00

La France est le pays dâ□□Europe qui a le plus faible taux dâ□□adoption (37%) de cette technologie au sein des entreprises qui nâ□□ont pas encore Ã©tÃ© victime de cyberattaque

Trellix, la sociÃ©tÃ© spÃ©cialiste de la cybersÃ©curitÃ© et pionniÃ¨re dans la dÃ©tection et la rÃ©ponse Ã©tendues (XDR), dÃ©voilait rÃ©cemment le second volet de son Ã©tude baptisÃ©e Â« Mind of the CISO : Behind the Breach Â».Â

Dans le cadre de ce rapport, elle a interrogÃ© plus de 500 responsables de la sÃ©curitÃ© des systÃ¨mes dâ□□information travaillant dans des entreprises de plus de 1000 employÃ©s afin de mieux comprendre les dÃ©fis auxquels ils sont confrontÃ©s aprÃ¨s avoir subi une cyberattaque.

La France se distingue des autres pays dâ□□Europe en ce que lâ□□adoption de technologies avancÃ©es telles que le XDR nâ□□intervient dans prÃ¨s dâ□□un cas sur 2 (43%) quâ□□aprÃ¨s avoir Ã©tÃ© victime dâ□□une cyberattaque majeure.

Le manque de technologie de pointe comme premiÃ¨re cybermenace

InterrogÃ©s sur la variable dâ□□ajustement principale suite Ã une cyberattaque, 70% des RSSI europÃ©ens sâ□□entendent sur le fait que les amÃ©liorations Ã introduire portent sur la technologie ou les technologies cyber dont leurs entreprises sont Ã©quipÃ©es.

ParticuliÃ¨rement Ã©levÃ© en France, ce pourcentage sâ□□Ã©tablit Ã 80%, dÃ©montrant un besoin accru d'investissements dans des technologies plus avancÃ©es. Pour la presque majoritÃ© des responsables sÃ©curitÃ© franÃ§ais (47%), la raison identifiÃ©e derriÃ¨re une cyberattaque dâ□□ampleur est celle d'une technologie qui n'Ã©tait pas Ã la hauteur. Par opposition, la premiÃ¨re raison invoquÃ©e par les RSSI anglais et allemands est l'incapacitÃ© Ã contenir rapidement, mÃªme aprÃ¨s sa dÃ©tection, un incident.

Les FranÃ§ais nâ□□hÃ©sitent pas Ã opÃ©rer des changements majeurs aprÃ¨s une cyberattaque

En France, une cyberattaque majeure conduit le plus souvent Ã une rÃ©Ã©valuation complÃ¨te de la stratÃ©gie cyber de l'entreprise tandis que dans le reste de lâ□□Europe, elle a le plus souvent seulement pour consÃ©quence lâ□□achat de solutions de cybersÃ©curitÃ© supplÃ©mentaires.

Synonyme de perturbations importantes pour les RSSI franÃ§ais, 47% dâ□□entre eux dÃ©clarent quâ□□une cyberattaque majeure a engendrÃ© des interruptions dâ□□activitÃ©, au sein de leur entreprise, soit le pourcentage le plus Ã©levÃ© dâ□□Europe. A cela sâ□□ajoute un stress supplÃ©mentaire important pour les Ã©quipes en charge de la cybersÃ©curitÃ©.

Les entreprises franÃ§aises sont aussi plus susceptibles que leurs homologues europÃ©ennes de changer de prestataire suite Ã une cyberattaque majeure (83% vs. 68% pour la moyenne europÃ©enne). En revanche, pour ceux qui nâ□□envisagent pas de changer, câ□□est le coÃ»t qui est Ã©voquÃ© comme premier frein (80%).

Vers une adoption du XDR

InterrogÃ©s plus en dÃ©tails sur les solutions technologiques dont ils disposaient avant vs. aprÃ¨s une cyberattaque majeure, on constate que le taux dâ□□adoption de certaines technologies clÃ©s telles que le XDR, le Endpoint ou le Threat Intelligence sont parmi les plus bas dâ□□Europe en France (respectivement, 40%, 27% et 40%). 43% des entreprises franÃ§aises se sont finalement Ã©quipÃ©es du XDR suite Ã une cyberattaque, 60% du Endpoint et 47% de la Threat Intelligence, des pourcentages plus Ã©levÃ©s que la moyenne europÃ©enne.

Parmi ceux qui nâ□□Ã©taient pas Ã©quipÃ©s dâ□□une solution XDR, 80% des RSSI franÃ§ais estiment que cette technologie aurait pu leur offrir une meilleure comprÃ©hension du paysage cyber actuel et des menaces Ã©mergentes.

En outre, 58% pensent quâ□□il y aurait eu moins dâ□□impact sur leur entreprise si le XDR avait Ã©tÃ© implÃ©mentÃ© et 80% dÃ©clarent que cela aurait Ã minima pu leur permettre de prÃ©venir la menace. Enfin, 93% des rÃ©pondants franÃ§ais dÃ©clarent avoir obtenu plus de soutien de leur direction aprÃ¨s une attaque.

Â« Lâ□□Ã©volution rapide des cybermenaces couplÃ©e Ã la pÃ©nurie de ressources va obliger les organisations Ã basculer dans le SOC du futur dont la remÃ©diation rapide est la pierre angulaire.

Le XDR sâ□□impose aujourd'hui comme une approche Ã valeur ajoutÃ©e permettant dâ□□obtenir cette visibilitÃ© indispensable Ã la mise en Å□uvre dâ□□une rÃ©ponse unifiÃ©e la plus rapide possible face Ã la complexitÃ© croissante des cybermenaces. Il reste toutefois beaucoup dâ□□efforts Ã faire car la perception de la puissance du XDR reste plus faible en France que dans le reste de lâ□□Europe Â», a dÃ©clarÃ© Adrien Vandeeweghe, Directeur France et BÃ©nÃ©lux de Trellix.Â